

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
United States Department of Justice, Federal Bureau)	
of Investigation and Drug Enforcement)	
Administration)	
)	RM-10865
Joint Petition for Rulemaking to Resolve Various)	
Outstanding Issues Concerning the Implementation)	
of the Communications Assistance for Law)	
Enforcement Act)	

COMMENTS OF LEAP WIRELESS INTERNATIONAL, INC.

Leap Wireless International, Inc., on behalf of its U.S. operating subsidiaries (collectively referred to as “Leap”), through counsel, hereby submits its initial Comments in the above-captioned proceeding. Leap supports Law Enforcement¹ in its efforts to preserve and protect the security and safety of the United States. However, Leap urges the Commission to decline to adopt the proposals set forth in Law Enforcement’s Petition for Rulemaking (“Petition”).

Leap is particularly concerned with two aspects of the Petition: (1) Law Enforcement’s efforts to expand the scope of CALEA to reach information services, which are explicitly excluded from the statute; and (2) Law Enforcement’s proposal that Law Enforcement not bear certain costs associated with its surveillance requests, but instead shift those costs onto carriers and their rate payers. Because these proposals are contrary to statute and would present unreasonable costs on telecommunications carriers and, possibly, their customers, the Commission should deny the Petition.

¹ For purposes of convenience, as used herein, “Law Enforcement” refers to the above-captioned petitioners as well as to law enforcement agencies generally.

I. INTRODUCTION

Leap is one of the original Entrepreneur's Block PCS providers. It is one of the few independent designated entities ("DEs"), unaffiliated with any large wireless incumbent. Leap has brought substantial and beneficial competition in both wireless and wireline telephony, and it has often been an important and independent voice in the wireless industry. Today, Leap, through its wholly owned subsidiary, Cricket Communications, Inc. ("Cricket"), provides wireless services to approximately 1.5 million customers in 39 markets across the United States.

Under its innovative "Cricket" branded service, Leap offers consumers unlimited, all-you-can-talk local service for a flat rate of roughly \$30 per month and recently began offering unlimited local and long distance plans at a slightly higher price point. This affordable and predictable service model has made wireless available to a broad group of under-served consumers, including blue-collar workers, the credit-challenged, and other consumer segments that many of the largest carriers have often left behind. Through superior service and its low and predictable flat-rated pricing, Leap not only presented a competitive challenge to other wireless carriers, but also offered customers a viable substitute for landline telephony.

II. THE STATUTE SPECIFICALLY EXCLUDES INFORMATION SERVICES, SUCH AS INTERNET ACCESS AND SHORT MESSAGING SERVICE, FROM CALEA

The Commission should deny Law Enforcement's request to expand the reach of CALEA to information services, which specifically are excluded from the statute, through either rulemaking or declaratory ruling.² In its Petition, Law Enforcement takes issue with the fact that "certain carriers have claimed to both the Commission and the FBI that their type of

² Petition at 7-33.

communications service is not subject to CALEA.”³ To the contrary, as was raised in earlier comments filed by the Cellular Telecommunications & Internet Association (“CTIA”), the problem does not lie with the carriers’ classification of their services but rather, “the FBI’s efforts to force CALEA into the information services domain.”⁴

“Information service” is defined as “the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications,” and specifically includes “electronic publishing” and “electronic messaging.”⁵ Wireless carriers typically provide multiple information services offerings, such as Internet access, short messaging services (“SMS”), digital picture phone service, wireless video game services, etc. Wireless carriers typically provide information services using the wireless infrastructure facilities over which they provide telecommunications services. Although such wireless facilities are subject to CALEA, they are not subject to the statute’s capability requirements “insofar as they are engaged in providing information services.”⁶ Similarly, under the statute, CALEA capability requirements “do not apply to . . . information services.”⁷

The Commission has confirmed that “where facilities are used to provide both telecommunications and information services . . . such joint-use facilities are subject to CALEA

³ *Id.* at 7.

⁴ Cellular Telecommunications & Internet Association Comments in Support of AT&T Wireless’ Petition for Extension of the Compliance Date, CC Docket No. 97-213, at 9 (filed Aug. 31, 2001) (“CTIA CALEA Extension Comments”).

⁵ 47 U.S.C. § 1001(6).

⁶ *Id.* § 1001(8)(C)(i).

⁷ *Id.* § 1002(b)(2)(A).

in order to ensure the ability to surveil the *telecommunications services*.”⁸ As such, to the extent that a telecommunications carrier’s facilities are subject to CALEA capability requirements, such requirements would apply only to the “telecommunications services” provided over those facilities. “The mere use of transmission facilities would not make the [information services] offering subject to CALEA.”⁹

Leap’s most popular information services feature is its text messaging service, commonly referred to as SMS. SMS is a prominent example of a service that falls squarely under the definition of information services, but which Law Enforcement nonetheless has sought CALEA compliance. CALEA’s definition of “information services” includes “electronic messaging services,” defined as “a software based services that enable the sharing of data, images, sound, writing, or other information among computing devices controlled by the senders or recipients of the messages.”¹⁰ Congress further explained:

The term “information services” includes messaging services offered through software such as groupware and enterprise or personal messaging software, that is, services based on products (including but not limited to multimedia software) of which Lotus Notes (and Lotus Network Notes), Microsoft Exchange Server, Novell Netware, CC: Mail, MCI Mail, Microsoft Mail, Microsoft Exchange Server, and AT&T Easylink (and their associated services) are both examples and precursors.

While SMS has evolved since CALEA was enacted, Congress anticipated the evolution of information services, and SMS is precisely the type of service that Congress intended to exclude from CALEA. The legislative history instructs:

⁸ *Communications Assistance for Law Enforcement*, 15 FCC Rcd 7105, at ¶ 27 (1999) (“Second Report and Order”) [emphasis added].

⁹ *Id.*

¹⁰ 47 U.S.C. 1001(4).

It is the Committee's intention not to limit the definition of "information services" to such current services, but rather to anticipate the rapid development of advanced software and to include such software services in the definition of "information services." By including such software-based electronic messaging services within the definition of information services, they are excluded from compliance with the requirements of the bill.

The statutory exemption for SMS could not be more clear. As described by CTIA, "SMS messages are created, sent, stored and retrieved by its customers. It is the quintessential 'electronic messaging' included in the definition of exempt information services."¹¹

Regardless of whether certain services are exempt from CALEA's requirements, however, Leap has a proven track record of striving to meet its obligations under various surveillance statutes.¹² CALEA's legislative history recognizes that, "information services can be wiretapped pursuant to court order, and their owners must cooperate when presented with a wiretap order, but these services and systems do not have to be designed so as to comply with the [CALEA] capability requirements."¹³ Indeed, information services and systems, including those already deployed by Cricket, have not been designed to permit data and content interception in the same manner as telecommunication services, and the platforms on which such information services operate have not been designed to interconnect with the Verint Communications interception platform that Cricket purchased to comply with CALEA. A rule that would subject information services to CALEA would be contrary to the plain meaning of the statute, and would unduly burden Leap and other wireless providers by requiring them to unwind, redesign, and redeploy their information systems and the CALEA interception platforms that they just

¹¹ CTIA CALEA Extension Comments at 8.

¹² For example, in its comments, CTIA noted that AT&T Wireless had committed to voluntarily deploy a solution for SMS intercepts. *Id.* at n.6.

¹³ H.R. Rep. No. 103-827(I), at 21, *reprinted in* 1994 U.S.C.C.A.N. 3489, 3498.

deployed to comply with CALEA, including the recently imposed Punchlist item requirements. Leap is concerned that Law Enforcement's most recent requests for additional CALEA requirements set forth in the Petition are part of a systematic effort to reallocate the entire burden of surveillance investigations onto private enterprise and, in turn, on the consumers. Leap reaffirms its continued intention to work with Law Enforcement to comply with all lawfully ordered surveillance requests, but Leap urges the Commission to protect consumers of wireless communications and require that Law Enforcement bear the appropriate technical and financial burden of communication interception surveillance.

III. LAW ENFORCEMENT SHOULD PROPERLY COMPENSATE CARRIERS COMPLYING WITH SURVEILLANCE REQUESTS

A. The Costs Associated With Compliance with Individual Surveillance Orders Are Substantial

The demands placed on Leap due to surveillance orders have skyrocketed over the last few years, well out of proportion to the increases in Leap's subscriber base. In addition to the capital costs of deploying, maintaining, and upgrading facilities to handle the ever-increasing volume of surveillance orders from Law Enforcement, Leap expends substantial employee resources on subpoena compliance.

As recently as January 2001, Law Enforcement's demands on Leap were fairly modest, approximately 10 to 20 subpoenas, and only one or two intercepts per month. At that time, Leap utilized only 10 to 20 percent of one employee's time to handle Law Enforcement subpoenas and other lawful requests. As Law Enforcement's demands have increased, Leap had to increase the number of staff dedicated to subpoena compliance in order to continue to respond in a timely fashion. During the first quarter of 2004, Law Enforcement requests have risen to an average of over 1,100 subpoenas/court orders per month (each subpoena typically including

multiple information requests), representing approximately 4,300 separate requests for subscriber information or calling history, and 44 requests for intercepts. In March 2004 alone, Cricket processed an average of 191 subpoena/court order requests each calendar day.

Today, Cricket employs one full-time Subpoena Compliance Manager and three (3) full-time Subpoena Analysts, whose sole responsibility is to handle subpoena compliance matters for the company. The Subpoena Compliance Manager and Analysts report to Senior Legal Counsel responsible for ensuring compliance consistent with applicable law. In addition, numerous Cricket engineers and technicians around the country are required to maintain the intercept facilities, answer phone calls from Law Enforcement and provide the assistance to implement, provision and trouble-shoot ordered intercepts. These engineers and technicians are pulled from their regular duties at various times throughout the day and night to respond to the average of over 158 Law Enforcement requests Cricket has received each calendar day during the first quarter of 2004. Cricket's excellent record of responsiveness to Law Enforcement is borne out by its average turn-around time for completion of subpoena requests of 16 to 18 days, and an average time of a half-day to implement an intercept following receipt of a court order. Leap understands these times to be well ahead of the industry average.

Leap's substantial efforts necessarily are not without costs. Leap estimates that implementation of surveillance requests and subpoena compliance costs Leap approximately \$1.45 million annually at an average cost per wiretap of \$3,973, including costs associated with capital expenditures, recurring costs (such as software maintenance), and staffing. In the interest of administrative expedience, Leap charges Law Enforcement a flat fee of \$2,200 for intercepts, approximately *half* of its total costs to comply with such surveillance requests. Also, Leap does not charge any further fee for converting an existing pen register to a wiretap intercept.

As discussed below, this discounted flat rate is completely in line with the statutory requirement that Law Enforcement “shall compensate” telecommunications carriers for providing “assistance or facilities.”¹⁴ The costs charged to Law Enforcement are not excessive, but accurately reflect the (discounted) costs of subpoena compliance. The Commission should consider the burdens placed on small carriers such as Leap to comply with surveillance requests, and deny Law Enforcement’s proposal to alter the current compensation scheme.

B. The Statute Provides for Cost Recovery from Law Enforcement

The Petition incorrectly claims that carriers may not recover from Law Enforcement the capital costs required to implement individual intercept requests and suggests that carriers instead should pass such costs through to their customers.¹⁵ However, the various statutes that require telecommunications carriers to assist Law Enforcement with surveillance requests and access to records all require that Law Enforcement, not consumers, have responsibility to compensate the carrier for such assistance.¹⁶ For example, Section 2518 of Title III states that “[a]ny provider of wire or electronic communications service . . . shall be compensated therefore *by the applicant [of the surveillance order]* for reasonable expenses incurred in providing such facilities or assistance.”¹⁷

The Commission has recognized that, pursuant to federal and state law, “carriers can recover at least a portion of their CALEA software and hardware costs by charging [Law Enforcement], for each electronic surveillance order authorized by CALEA, a fee that includes

¹⁴ 18 U.S.C. § 2518.

¹⁵ Petition at 69.

¹⁶ See 18 U.S.C. § 2518 (Omnibus Crime Control and Safe Streets Act of 1968 (“Title III”), *id.* § 2706 (Electronic Communications Privacy Act (“ECPA”); 50 U.S.C. §§ 1802, 1842 (Foreign Intelligence Surveillance Act (“FISA”).

¹⁷ 18 U.S.C. § 2518.

recovery of capital costs, as well as recovery of the specific costs associated with each order.”¹⁸

Although CALEA generally does not mandate that Law Enforcement pay for the initial compliance of post-January 1, 1995 switches,¹⁹ the statute does not preclude carriers from recovering capital costs and specific variable costs from Law Enforcement that are associated with individual intercept requests. These costs are “reasonable expenses incurred in providing . . . facilities and assistance” to be reimbursed by Law Enforcement under various federal and state surveillance statutes.

If Law Enforcement were permitted to discontinue compensating Leap for subpoena compliance, Leap’s business of providing quality, low-cost wireless services would be jeopardized. As a relatively small wireless carrier focusing on affordable services, Leap could not shoulder on its own the tremendous costs associated with such compliance, nor is it a viable alternative for Leap’s customer base to absorb these costs through rate increases. Leap will, of course, respond with due speed to surveillance orders, but without reasonable compensation from Law Enforcement, Leap’s ability to continue to provide the dedicated equipment and staff required to carry out certain surveillance activities may no longer be “reasonably achievable” under the statute.

¹⁸ *Communications Assistance for Law Enforcement Act*, Order on Remand, 17 FCC Rcd 6896, ¶ 60 (2002) (citing 47 U.S.C. § 229(e) “and collateral state regulations”).

¹⁹ 47 U.S.C. § 109.

IV. CONCLUSION

For the foregoing reasons, the Commission should deny Law Enforcement's
Petition Rulemaking.

Respectfully submitted,

LEAP WIRELESS INTERNATIONAL, INC.

Laurie Itkin, Director, Government Affairs
Darren Brooks, Senior Legal Counsel
LEAP WIRELESS INTERNATIONAL, INC.
10307 Pacific Center Court
San Diego, CA 92121

/s/
James H. Barker
Jeffrey A. Marks
LATHAM & WATKINS, LLP
555 Eleventh Street, N.W., Suite 1000
Washington, D.C. 20004
(202) 637-2200

Its Counsel

April 12, 2004